

Online Status Protocols

Peter Williams,
ValiCert, Inc.

An Internet First?

- Where did OCSP technology originate?
- A threat of ECPA prosecution can be used to address violation of certificate policy
- A CA has duty to protect users from security compromise, including CPS failures
- IETF's OCSP v1 is about authoritative validation, not mere status signaling

FPMA First

- FPMA makes authoritative determinations concerning policy equivalence
- BCA issues and manages inter-domain certificates to signal determination status
- Agencies obtain and maintain good standing of their accreditation status with the PMA
- Relying Party liability assumed by NTIS

Status Technologies

- Move a Certificate to a “suspended” attribute in the (authoritative) Notice Repository. Perform LDAP compare operation.
- Update a CRL at the appropriate distribution point
- Issue a fresh, Signed OCSP Response

Review of Standards

- Request for Status on identified object(s)
- Response of authoritative designation(s)
- OCSP-specific Policy-based semantics
- OCSP Liabilities for mis-representation of status
- Message extensions permit notice indication and policy management

Four Corners

- A PKI has 4 elements:
 - Originator's NA/CA/RP Providers
 - A Message Originator
 - Recipient's NA/CA/RP Providers
 - the Message Recipient
- Validation occurs at the Recipient RP, as supported by the Originator's RP.

Validation Authority

- The role of the VA
- Is the VA Provider...
 - A value-added Repository service?
 - A value-added network interchange service?
- Yes and No. A VA is a distributed, authoritative repository.

BCA Validation Policy

- The certification semantics of the BCA concern good standing of an Agencies policy registration status with the FPMA
- the VA element of the BCA communicates the current designation of the identified object
- Validation Policy controls use and reliance of designations.

Finally

- ValiCert provision of the Public Validation Service rely upon the securities of the distributed ValiCert Validation System.
- The PVS availability design features push-based, multi-mastering technology, and a service access point locating protocol.
- The CRT-based “indexing” service is integrated with ValiCert EVA Products, which perform local OCSP.